Copyrights by ITEC,inc. 2025

令和７年度春期　情報処理安全確保支援士　午後試験　解答速報

（株）アイテック　IT 人材教育研究部　2025.4.23 発表

問１　サプライチェーンのリスク対策

【解答例】

［設問１］

(1) 上流の要件定義や設計工程において，セキュリティ要件や機能を作り込む考え方

(2) 業務委託先に求めるセキュリティ管理の要件と同等の内容を再委託契約に含め，L 社が事前に承認すること

［設問２］

(1) サーバ T ではない，システム Q を構成するサーバ上に配置する。

(2) 古いWebブラウザからのリクエストに対してサポート終了の旨のエラー画面を返す。

(3) 項番：1

修正内容：システムが利用する外部のスクリプトを情報資産に追加する。

［設問３］

(1) ア：10　　イ：4　　ウ：5　　エ：11

(2) a：共用アカウントを利用しており，必要な利用者にだけ発行されていない。

b：問題なし。

c：インシデント対応手順書は作成されている。

［設問４］

ソフトウェア構成について，利用されている部品を含めて自動で更新できるから。

［設問５］

(1) d：踏み台サーバ

(2)（あ）より早い段階で検査することによって，手戻りを少なくできる。

（い）ワークフローを構成することによって，チェックを自動化できる。

Copyrights by ITEC,inc. 2025

問２　脆弱性管理

【解答例】

［設問１］

a：ア　　b：ア　　c：ア　　d：ア　　e：イ

［設問２］

f：新たに報告された脆弱性への対応漏れ

g：セキュリティ維持に必要な設定変更の遅れ

［設問３］

(1) ウ

(2) サイト上の OpenSSH のログをツールで監視し，“Timeout before authentication”のメッセージがしきい値を超えて多数出力された場合にサイト担当者にアラート通知する。

(3) TLS クライアント認証を導入する。

［設問４］

(1) WA-1：item の数字 5 桁を変更する操作で済み，本来閲覧できない商品とも合致しやすいから。

WA-2：管理者用アカウントでのログイン，又は発注確認機能の URL の推測が難しいから。

(2) 3

［設問５］

(1) 現状値：利用者側で脅威情報を確認し，スコアを算出することが必要になるから。

EPSS 値：FIRST がスコア値を日次で算出し，公表しているから。

(2) l：EPSS スコアの収集

(3) 実際に悪用される脆弱性への対応を取りこぼさずに済むから。

［設問６］

m：A　　n：A　　o：C　　p：A　　q：B　　r：B　　s：A　　t：S

Copyrights by ITEC,inc. 2025

問３　スマートフォン用アプリケーションプログラムの開発

【解答例】

［設問１］

(1) HTTP リクエストの Authorization ヘッダーに指定された値を読み取る。

(2) F アプリを解析してコード中に定数として定義された AES-CBC の共通鍵及び初期ベクトルを取得し, F アプリのリソースから取得した暗号化されたアクセスキーを復号する。

(3) URL パスの e-service/nnnnnnnn.zip の注文番号箇所を 00000001 から 99999999 まで変えながら GET リクエストを送信する。

(4) https:// www.a-sha.co.jp.k-sha.co.jp

［設問２］

(1) www.a-sha.co.jp

(2) a：オ　b：ケ　c：ウ　d：コ　e：ア　f：イ　g：カ　h：キ

(3) 通信解析ツールのプライベート認証局の証明書を信頼されたルート証明書とする設定

［設問３］

i：(い)

［設問４］

(1) 接続先 URL を目視で確認できない問題

(2) F-URL のクエリパラメータ中の FQDN が www.a-sha.co.jp 以外の場合には通信を中断してエラー処理を行う機能

Copyrights by ITEC,inc. 2025

問４　IT 資産管理及び脆弱性管理

【解答例】

［設問１］

サーバ名：権威 DNS サーバ

変更内容：当該 CDN の Web サーバに関わる CNAME レコードの削除

［設問２］

(1) a：他社データセンターを契約して利用している

b：レンタルサービスを契約して利用している

(2) c：WHOIS

(3) あ：Z　　い：X　　う：Y

(4) d：オ　　e：ア　　f：イ　　g：ク　　h：キ

［設問３］

(1) ポートスキャナーを利用して開放ポートへの SSH 及び HTTP 接続可否を確認する。

(2) Z サービスを利用して利用 OS 及び SW のバージョンに関する情報を検索する。

(3) する場合：サービスの停止と切離しを行い，必要な脆弱性対応の措置を実施する。

しない場合：サービスの停止と切離しを行い，契約終了の手続きをとる。

［設問４］

(1) 4.0

(2) ウ

(3) 悪用の証拠があるか攻撃が観測されている。

(4) 項番 1：情シ部は，サーバの導入 SW の脆弱性情報を収集し，対策の優先度を判断の上，チケットを作成して事業部へ通知する。

項番 2：事業部は，脆弱性対応の措置を実施し，チケットにて情シ部へ報告する。

以上